JTSB-537

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-085472
(43)Date of publication of application : 30.03.1999

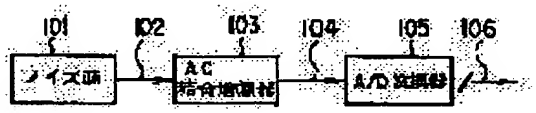
(51)Int.CI. G06F 7/58
G09C 1/00
H04L 9/26

(21)Application number : 09-249109
(22)Date of filing : 12.09.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : ONODERA TORU
KANEMOTO SHIGERU
SUMIYAMA SHIGEAKI

(54) PHYSICAL RANDOM NUMBER GENERATION DEVICE AND METHOD THEREFOR, AND PHYSICAL RANDOM NUMBER RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To increase the generating speed of physical random numbers and also to secure the good characteristics for the random numbers by providing the random number data based on the digital value which are converted by an A/D conversion means.
SOLUTION: Noise signals 102 which are generated from a noise source 101 due to a random event are amplified up to the conversion range of an A/D converter 105 by an AC coupling amplifier 103. Thus, the digital data are obtained and the random number data are generated from the digital data. A piece of random number data is obtained via a single conversion operation by applying the A/D conversion to the amplified signals 102 not by counting the random pulses of signals 102. Furthermore, the random number data of many bits are generated by the converter 105 and in a single A/D conversion operation. Thus, it is possible to obtain the random number data having no periodicity, to fast generate the physical random numbers and also to simplify the circuit constitution.



LEGAL STATUS

[Date of request for examination] 03.10.1997
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2980576
[Date of registration] 17.09.1999

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号

第2980576号

(45)発行日　平成11年(1999)11月22日　(24)登録日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ
Ｈ０４Ｌ　9/26		Ｈ０４Ｌ　9/00	６５９

請求項の数24(全 21 頁)

(21)出願番号　特願平9－249109

(22)出願日　平成９年(1997)９月12日

(65)公開番号　特開平11－85472

(43)公開日　平成11年(1999)３月30日

審査請求日　平成９年(1997)10月３日

早期審査対象出願

(73)特許権者　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　小野寺　徹
神奈川県川崎市幸区小向東芝町１番地
株式会社東芝研究開発センター内

(72)発明者　兼本　茂
神奈川県横浜市磯子区新杉田町８番地
株式会社東芝横浜事業所内

(72)発明者　角山　茂章
神奈川県川崎市幸区小向東芝町１番地
株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦　(外６名)

審査官　石田　信行

最終頁に続く

(54)【発明の名称】　物理乱数発生装置及び方法並びに物理乱数記録媒体

(57)【特許請求の範囲】

【請求項１】　ノイズ信号を出力するノイズ源と、
前記ノイズ信号を交流結合により直流分を除去しつつ増幅するＡＣ結合増幅手段と、
前記ＡＣ結合増幅手段により増幅された増幅ノイズ信号をＡ／Ｄ変換する，２ビット以上の精度を有して２ビット以上のビットデータに変換するＡ／Ｄ変換手段と、
前記Ａ／Ｄ変換手段により変換された２ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて２ビット以上の乱数データを提供する加工手段とを備えたことを特徴とする物理乱数発生装置。

【請求項２】　前記Ａ／Ｄ変換手段により変換されたディジタル値の平均値を、前記Ａ／Ｄ変換前若しくは前記Ａ／Ｄ変換後のデータに加えるオフセット調整手段を備えたことを特徴とする請求項１記載の物理乱数発生装置。

【請求項３】　前記Ａ／Ｄ変換手段は６ビット以上の精度を有し、変換されたディジタル値を構成する６ビット以上のビットデータのうち、上位から５ビット目以降の２つ以上のビットデータを取り出して乱数データとすることを特徴とする請求項１又は２記載の物理乱数発生装置。

【請求項４】　前記変換されたディジタル値の頻度分布が平均Ｎ、分散σ^2の正規分布となるとき、前記変換されたディジタル値がＮ±σ以上の範囲に入る場合のみを有効とすることを特徴とする請求項１乃至３記載のうち何れか１項記載の物理乱数発生装置。

【請求項５】　前記Ａ／Ｄ変換手段が出力する２以上の前記変換されたディジタル値を加算平均する微分非直線

性改善手段を備えたことを特徴とする請求項１乃至４記載のうち何れか１項記載の物理乱数発生装置。

【請求項６】　前記Ａ／Ｄ変換手段の入力値に微分非直線性改善用データをオフセットとして加算するとともに、前記微分非直線性改善用データに相当する改善用デジタルデータを前記Ａ／Ｄ変換手段の出力値から減算する微分非直線性改善手段を備えたことを特徴とする請求項１乃至４記載のうち何れか１項記載の物理乱数発生装置。

【請求項７】　前記ノイズ源は、熱雑音を前記ノイズ信号として使用することを特徴とする請求項１乃至６記載のうち何れか１項記載の物理乱数発生装置。

【請求項８】　前記ノイズ源は、抵抗の熱雑音を前記ノイズ信号として使用することを特徴とする請求項１乃至６記載のうち何れか１項記載の物理乱数発生装置。

【請求項９】　前記ノイズ源は、半導体素子の熱雑音を前記ノイズ信号として使用することを特徴とする請求項１乃至６記載のうち何れか１項記載の物理乱数発生装置。

【請求項１０】　前記ノイズ源は、フォトマルチプライヤの光電変換面の熱雑音を前記ノイズ信号として使用することを特徴とする請求項１乃至６記載のうち何れか１項記載の物理乱数発生装置。

【請求項１１】　前記ノイズ源は、真空管の陰極より発生する熱雑音を前記ノイズ信号として使用することを特徴とする請求項１乃至６記載のうち何れか１項記載の物理乱数発生装置。

【請求項１２】　前記ノイズ源は、真空マイクロ素子により発生する電子のゆらぎを前記ノイズ信号として使用することを特徴とする請求項１乃至６記載のうち何れか１項記載の物理乱数発生装置。

【請求項１３】　前記ノイズ源を高温で一定に保つ恒温手段を備えたことを特徴とする請求項７乃至１１記載のうち何れか１項記載の物理乱数発生装置。

【請求項１４】　前記乱数データに基づくデータを表示する表示手段を備えたことを特徴とする請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置。

【請求項１５】　前記乱数データを用いて信号を変調する信号変調手段を備えたことを特徴とする請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置。

【請求項１６】　前記乱数データを用いてデータの暗号化を行う暗号化手段を備えたことを特徴とする請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置。

【請求項１７】　前記請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置と、
前記物理乱数発生装置からの乱数データをコンピュータに入力可能に構成された，前記コンピュータのデータ入出力バスとのインターフェイス手段とを備えたことを特徴とする物理乱数入力装置。

【請求項１８】　前記請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置と、
前記物理乱数発生装置からの乱数データをコンピュータの要求に応じてコンピュータ・ネットワークに送出可能に構成された，前記コンピュータ・ネットワークとのインターフェイス手段とを備えたことを特徴とする物理乱数入力装置。

【請求項１９】　生成された乱数データを記録する記憶手段を備え、
乱数出力要求があった場合に、この要求に応じて乱数データを供給することを特徴とする請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置。

【請求項２０】　前記請求項１乃至１３記載のうち何れか１項記載の物理乱数発生装置により生成された乱数データを記録したことを特徴とする物理乱数記録媒体。

【請求項２１】　記録された乱数データについての検定方法及び又は検定結果を記録したことを特徴とする請求項２０記載の物理乱数記録媒体。

【請求項２２】　ノイズ源からノイズ信号を出力するステップと、
前記ノイズ信号を交流結合により直流分を除去しつつ増幅するＡＣ結合増幅ステップと、
前記ＡＣ結合増幅ステップにおいて増幅された増幅ノイズ信号をＡ／Ｄ変換する，２ビット以上の精度を有して２ビット以上のビットデータに変換するＡ／Ｄ変換ステップと、
前記Ａ／Ｄ変換ステップにより変換された２ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて２ビット以上の乱数データを提供するステップとを有することを特徴とする物理乱数発生方法。

【請求項２３】　前記Ａ／Ｄ変換手段の入力信号が変換範囲を超えたときに無効とし、変換範囲を超えずに変換されたディジタル値を乱数データとすることを特徴する請求項１乃至４記載のうち何れか１項記載の物理乱数発生装置。

【請求項２４】　前記加工手段は、
補正信号をＤ／Ａ変換して前記Ａ／Ｄ変換手段への入力前の値に加算し、かつ、前記補正信号を前記Ａ／Ｄ変換手段の出力から差し引くことで乱数データに加工する手段、
又は、　前記Ａ／Ｄ変換手段から別々に出力されるＡ／Ｄ変換値同士、若しくは前記Ａ／Ｄ変換手段の出力と前記Ａ／Ｄ変換の出力以外のランダムなデータを、加算（排他ＯＲ）して乱数データに加工する手段、
の何れかであることを特徴する請求項１乃至１６記載のうち何れか１項、又は請求項１９項、若しくは請求項２３項記載の物理乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は物理乱数発生装置及び方法並びに記録媒体、更に詳しくは汎用のコンピュータからパソコンやゲーム機のような民生レベルまで幅広い分野へ適用される物理乱数発生装置及び方法に関するものである。

【０００２】

【従来の技術】物理乱数とは、自然界のランダム現象を利用して作成された乱数のことを言い、代表的なランダム現象としては、放射線の発生や熱雑音のゆらぎ等が挙げられる。

【０００３】従来の物理乱数発生装置では、ノイズ源として放射線や熱雑音を用い、ノイズ源から発生するランダム・パルスの発生間隔または発生頻度を測定している。

【０００４】例えば、単位時間当たりの放射線の発生個数を何度も測定し、測定値の頻度分布を作成すると平均Ｎ、標準偏差$N^{1/2}$の正規分布に近づく。すなわち、１００回の測定を行った場合、そのうち９９回は、Ｎ－３$N^{1/2}$からＮ＋３$N^{1/2}$のいずれかの値になる。測定値の頻度分布は正規分布なので、このまま正規分布乱数として用いることができるが、一般的には分布が一様な方が便利なことが多いため正規分布を一様乱数に変換する必要がある。

【０００５】そこで、従来装置では、正規分布から一様乱数を得るために、計数結果の最下位桁の値だけを用いて頻度分布形状に依存しない乱数としている。さらに、得られた計数値の最下位桁として１ビットの値を用いることにより、計測結果を偶数または奇数の２通りに分類することができ、Ｎが十分に大きければ各々の発生頻度は５０％になり、乱数としての性質が向上する。

【０００６】従来装置では、このような１ビットの乱数データ発生回路を複数個用意することにより、多ビットの乱数データを発生している。このような従来技術は、例えば石田正次氏の「モンテカルロ法と乱数」（科学基礎論研究１７．２．２９（１９６５））等に記載されている。

【０００７】

【発明が解決しようとする課題】しかし、上述したような従来の一様な物理乱数発生方法では、計数ノイズ信号から乱数データを得るためには、Ｎ（１００～２００）個のノイズ信号を計数しなければならないため、１個の乱数を発生するために多くの時間が必要となるという課題がある。

【０００８】また、計数結果として１つのノイズ源から発生できる乱数データは１ビットのため、たとえば、計算機が扱う最小単位であるバイト単位の乱数データを発生するためには、８つの互いに相関のないノイズ源と８系統の乱数発生回路が必要になる。これは装置の小型化・低価格化を実現するために解決されるべき課題である。

【０００９】このような課題のため、物理乱数発生装置から発生する乱数データを用いた膨大なシミュレーションを行う場合、計算機にいかに高速なＣＰＵを搭載しても、計算結果が得られる時間が乱数発生速度に依存するためシミュレーションの高速化を実現できないという状況となっていた。

【００１０】また、１バイトの乱数を発生するために８系統のノイズ源と処理回路が必要となるため装置が大がかりな物となり、これが低価格化を阻害し、物理乱数発生装置の普及を阻む要因となつている。

【００１１】一方、高速かつ安価な従来から物理乱数発生装置が実現されれば、シミュレーション、知能関連の研究、ネットワーク上のセキュリティー研究等の科学技術計算分野や、通信機器分野（通信データのセキュリティー、変調の暗号化等の通信機器分野のみならず、パチンコ台の出玉確率、一般のゲーム機等のゲーム機分野等にも利用されることが考えられる。

【００１２】本発明は、このような実情を考慮してなされたもので、物理乱数発生速度を向上するとともに、乱数として良質な特性を有する物理乱数を提供し、さらには汎用のコンピュータからパソコンやゲーム機のような民生レベルまで幅広い分野への適用をできるようにした物理乱数発生装置及び方法、物理乱数入力装置並びに物理乱数記録媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】上記課題を解決するために、請求項１に対応する発明は、ノイズ信号を出力するノイズ源と、ノイズ信号を交流結合により直流分を除去しつつ増幅するＡＣ結合増幅手段と、ＡＣ結合増幅手段により増幅された増幅ノイズ信号をＡ／Ｄ変換する，２ビット以上の精度を有して２ビット以上のビットデータに変換するＡ／Ｄ変換手段と、前記Ａ／Ｄ変換手段により変換された２ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて２ビット以上の乱数データを提供する加工手段とを備えた物理乱数発生装置である。本発明は、このような手段を設け、直流成分が除去された増幅信号をＡ／Ｄ変換しているので、Ａ／Ｄ変換されたディジタル値の各ビットはそのままビット単位の乱数データとして取り扱い可能になっている。したがって、計数ノイズ信号から乱数データを得るのに、多数のノイズ信号を計数する必要がなくなり、１個の乱数を発生させるのに必要な時間を極めて短くすることができる。また、ノイズ源及び乱数発生処理回路を簡素化することができ、ひいては物理乱数発生装置の低価格化にも寄与する。また、一度に２ビット以上の乱数データを得ることができ、より一層多数の乱数データを短時間で提供することができる。さらに、Ａ／Ｄ変換手段からのビットデータを微分非直線性を改善する加工手段を用いて加工するようにしているので、たとえ一度に２ビット以上の乱数データを取り出しても十分

に精度の高い乱数を得ることができる。また、請求項２に対応する発明は、請求項１に対応する発明において、Ａ／Ｄ変換手段により変換されたディジタル値の平均値を、Ａ／Ｄ変換前若しくはＡ／Ｄ変換後のデータに加えるオフセット調整手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１に係る発明と同様な作用効果が得られる他、Ａ／Ｄ変換手段からの出力は多くの場合、その頻度分布が正規分布あるいはこれに近い分布に従うと考えられるため、この変換されたディジタル値の平均値をオフセットとして加えることで、より完全に直流成分を除去することができ、良質な乱数とすることができる。さらに、請求項３に対応する発明は、請求項１又は２に対応する発明において、Ａ／Ｄ変換手段は６ビット以上の精度を有し、変換されたディジタル値を構成する６ビット以上のビットデータのうち、上位から５ビット目以降の２つ以上のビットデータを取り出して乱数データとする物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１又は２に係る発明と同様な作用効果が得られる。また、Ａ／Ｄ変換手段からの出力は多くの場合、その頻度分布が正規分布あるいはこれに近い分布に従うと考えられ、さらにこの場合、後述するシミュレーション結果よれば５ビット目以降のデータのときに確実に一様性が高くなるので、より一層良質な乱数データとすることができる。さらにまた、請求項４に対応する発明は、請求項１～３に対応する発明において、変換されたディジタル値の頻度分布が平均Ｎ、分散σ^2の正規分布となるとき、変換されたディジタル値がＮ±σ以上の範囲に入る場合のみを有効とする物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～３に係る発明と同様な作用効果が得られる他、変換されたディジタル値の有効範囲をＮ±σ以上の範囲とすることで、上位ビットまでその一様性を確実に担保することができ、変換されたディジタル値が多数ビットの場合でも全ビットについて良質な乱数データとして使用することができる。一方、請求項５に対応する発明は、請求項１～４に対応する発明において、Ａ／Ｄ変換手段が出力する２以上の変換されたディジタル値を加算平均する微分非直線性改善手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～４に係る発明と同様な作用効果が得られる他、Ａ／Ｄ変換手段に由来する微分非直線性を改善して良質な乱数データとすることができる。次に、請求項６に対応する発明は、請求項１～４に対応する発明において、Ａ／Ｄ変換手段の入力値に微分非直線性改善用データをオフセットとして加算するとともに、微分非直線性改善用データに相当する改善用デジタルデータをＡ／Ｄ変換手段の出力値から減算する微分非直線性改善手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～４に係る発明と同様な作用効果が得られる他、Ａ／Ｄ変換手段に由来する微分非直線性を改善して良質な乱数データとすることができる。また、請求項７に対応する発明は、請求項１～６に対応する発明において、ノイズ源は、熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～６に係る発明と同様な作用効果が得られる他、熱雑音に基づく一様性の高い乱数データを提供することができる。さらに、請求項８に対応する発明は、請求項１～６に対応する発明において、ノイズ源は、抵抗の熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項８に係る発明と同様な作用効果を得ることができる。さらにまた、請求項９に対応する発明は、請求項１～６に対応する発明において、ノイズ源は、半導体素子の熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項８に係る発明と同様な作用効果を得ることができる。一方、請求項１０に対応する発明は、請求項１～６に対応する発明において、ノイズ源は、フォトマルチプライヤの光電変換面の熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項８に係る発明と同様な作用効果を得ることができる。次に、請求項１１に対応する発明は、請求項１～６に対応する発明において、ノイズ源は、真空管の陰極より発生する熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項８に係る発明と同様な作用効果を得ることができる。また、請求項１２に対応する発明は、請求項１～６に対応する発明において、ノイズ源は、真空マイクロ素子により発生する電子のゆらぎをノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～６に係る発明と同様な作用効果が得られる他、電子のゆらぎに基づく一様性の高い乱数データを提供することができる。さらに、請求項１３に対応する発明は、請求項７～１１に対応する発明において、ノイズ源を高温で一定に保つ恒温手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項７～１１に係る発明と同様な作用効果が得られる他、ノイズ源を安定な熱雑音発生状態に保ち、安定なノイズ信号発生により安定した乱数データの提供を行うことができる。さらにまた、請求項１４に対応する発明は、請求項１～１３に対応する発明において、乱数データに基づくデータを表示する表示手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～１３に係る発明による高速で良質な乱数データに基づくデータを表示することを可能とした簡素かつ高性能で低価格な装置を提供することができる。一方、請求項１５に対応する発明は、

請求項１～１３に対応する発明において、乱数データを用いて信号を変調する信号変調手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～１３に係る発明による高速で良質な乱数データを用いて信号を変調することを可能とした簡素かつ高性能で低価格な装置を提供することができる。次に、請求項１６に対応する発明は、請求項１～１３に対応する発明において、乱数データを用いてデータの暗号化を行う暗号化手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～１３に係る発明による高速で良質な乱数データを用いてデータの暗号化を行うことを可能とした簡素かつ高性能で低価格な装置を提供することができる。また、請求項１７に対応する発明は、請求項１～１３記載のうち何れか１項記載の物理乱数発生装置と、物理乱数発生装置からの乱数データをコンピュータに入力可能に構成された，コンピュータのデータ入出力バスとのインターフェイス手段とを備えた物理乱数入力装置である。本発明は、このような手段を設けたので、請求項１～１３に係る発明による高速で良質な乱数データをコンピュータに入力することができる。また、この装置の形態として例えば基板形態又はカード形態の装置が考えられる。さらに、請求項１８に対応する発明は、請求項１～１３記載のうち何れか１項記載の物理乱数発生装置と、物理乱数発生装置からの乱数データをコンピュータの要求に応じてコンピュータ・ネットワークに送出可能に構成された，コンピュータ・ネットワークとのインターフェイス手段とを備えた物理乱数入力装置である。本発明は、このような手段を設けたので、請求項１～１３に係る発明による高速で良質な乱数データを、要求に応じネットワークを介してコンピュータに入力することができる。さらにまた、請求項１９に対応する発明は、請求項１～１３に対応する発明において、生成された乱数データを記録する記憶手段を備え、乱数出力要求があった場合に、この要求に応じて乱数データを供給する物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～１３に係る発明と同様な作用効果が得られる他、要求がないときには生成した乱数を記憶手段に蓄え、要求時にこの蓄えた乱数を出力することで、安定的な乱数の供給を可能とすることができる。一方、請求項２０に対応する発明は、請求項１～１３記載のうち何れか１項記載の物理乱数発生装置により生成された乱数データを記録した物理乱数記録媒体である。本発明は、このような手段を設けたので、請求項１～１３に係る発明による高速で良質な乱数データを記録媒体により提供することができる。次に、請求項２１に対応する発明は、請求項２０に対応する発明において、記録された乱数データについての検定方法及び又は検定結果を記録した物理乱数記録媒体である。本発明は、このような手段を設けたので、請求項２０に係る発明と同様な作用効果が得られる他、その乱数データに対する信頼性を高めることができる。さらに、請求項２２に対応する発明は、ノイズ源からノイズ信号を出力するステップと、ノイズ信号を交流結合により直流分を除去しつつ増幅するＡＣ結合増幅ステップと、ＡＣ結合増幅ステップにおいて増幅された増幅ノイズ信号をＡ／Ｄ変換する，２ビット以上の精度を有して２ビット以上のビットデータに変換するＡ／Ｄ変換ステップと、前記Ａ／Ｄ変換ステップにより変換された２ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて２ビット以上の乱数データを提供するステップとを有する物理乱数発生方法である。本発明は、このような手段を設けたので、請求項１に係る発明と同様な作用効果を得ることができる。さらにまた、請求項２３に対応する発明は、請求項１～４に対応する発明において、Ａ／Ｄ変換手段の入力信号が変換範囲を超えたときに無効とし、変換範囲を超えずに変換されたディジタル値を乱数データとする物理乱数発生装置である。本発明は、このような手段を設けたので、請求項１～４に係る発明と同様な作用効果を得ることができる他、より良質な乱数データを得ることができる。次に、請求項２４に対応する発明は、請求項１～１６、１９又は２３に対応する発明において、加工手段は、補正信号をＤ／Ａ変換してＡ／Ｄ変換手段への入力前の値に加算し、かつ、補正信号を前記Ａ／Ｄ変換手段の出力から差し引くことで乱数データに加工する手段、又は、Ａ／Ｄ変換手段から別々に出力されるＡ／Ｄ変換値同士、若しくはＡ／Ｄ変換手段の出力とＡ／Ｄ変換の出力以外のランダムなデータを、加算（排他ＯＲ）して乱数データに加工する手段、の何れかである物理乱数発生装置である。

【００１４】
【００１５】
【００１６】
【００１７】
【００１８】
【００１９】
【００２０】
【００２１】
【００２２】
【００２３】
【００２４】
【００２５】
【００２６】
【００２７】
【００２８】
【００２９】
【００３０】
【００３１】
【００３２】
【００３３】

【００３４】
【００３５】
【００３６】
【００３７】
【００３８】
【００３９】
【００４０】
【００４１】
【００４２】
【００４３】
【００４４】
【００４５】
【００４６】
【００４７】
【００４８】
【００４９】
【００５０】
【００５１】
【００５２】
【００５３】
【００５４】
【００５５】
【００５６】
【００５７】
【００５８】
【００５９】
【００６０】
【００６１】
【００６２】
【発明の実施の形態】以下、本発明の実施の形態について説明する。
【００６３】（発明の第１の実施の形態）図１は本発明の第１の実施の形態に係る物理乱数発生装置の構成例を示すブロック図である。
【００６４】この物理乱数発生装置においては、ノイズ源１０１からのノイズ信号１０２がＡＣ結合増幅器１０３に入力され、その増幅されたノイズ信号１０４がアナログ・ディジタル変換器１０５にてＡ／Ｄ変換されて乱数データ１０６として出力されるようになっている。ここで、アナログ・ディジタル変換器１０５は、１ビットあるいは２ビット精度以上のＡ／Ｄ変換器である。
【００６５】図２は本実施形態の物理乱数発生装置におけるＡＣ結合増幅器の内部構成例を示す図である。
【００６６】ＡＣ結合増幅器１０３は、交流結合により信号の直流成分を通過させないようにしつつ増幅を行う部分であり、ノイズ信号１０２を入力する入力コンデンサ１８０１と、入力コンデンサ１８０１の出力信号を増幅して出力コンデンサに入力する増幅器１８０２と、増幅されたノイズ信号１０４を出力する出力コンデンサ１８０３とによって構成されている。
【００６７】次に、以上のように構成された本発明の実施の形態に係る物理乱数発生装置の動作について説明する。
【００６８】まず、ノイズ源１０１からランダム事象に起因するノイズ成分が出力されるが、そのノイズ信号波形例を図３に示す。
【００６９】図３はノイズ信号波形の例を示す図である。
【００７０】使用するノイズ源１０１にもよるが、ノイズ信号波形はオフセット１７０１電圧（または電流）とその回りに分布するノイズ成分１７０２の加算合成された波形となる。
【００７１】一般的にノイズ源１０１から得られるノイズ成分のレベルが小さいので、大きな増幅度を有する増幅器を用いてノイズ信号１０２を増幅する必要がある。しかし、オフセット１７０１と共に増幅すると増幅器の出力信号が飽和して動作しなくなる。そこで、増幅回路としてＡＣ結合増幅器１０３が使用され、オフセット１７０１を除いたノイズ成分１７０２のみが増幅される。
【００７２】すなわち図２に示すＡＣ結合増幅器１０３では以下のような増幅動作がなされる。
【００７３】まず、入力コンデンサ１８０１により、ノイズ信号１０２のオフセット１７０１が除かれ、増幅器１８０２によりノイズ成分１７０２のみが増幅される。さらに、出力コンデンサ１８０３により、増幅器１８０２自身が有するオフセットを増幅した直流電圧が、増幅されたノイズ信号１０４に含まれないように除去される。
【００７４】したがって、増幅されたノイズ信号１０４は、ＡＣ結合によりオフセットが０で、０の回りにノイズ成分が均等に分布する波形となっている。
【００７５】たとえば、増幅されたノイズ信号１０４を１ビット精度のアナログ・ディジタル変換器１０５を用いてディジタル値に変換すると、増幅されたノイズ信号１０４の極性に応じて０または１の値となる。ノイズ源から得られる信号はランダムであるから、０または１の値になる順番は確定しない。また、ＡＣ結合されているから、０になる確率と１になる確率が等しい。すなわち一様性があり周期性のない質の良い１ビットの乱数データを取得することができる。
【００７６】これは、単純なレベルコンパレータを用いて実現できる１ビット乱数データである。さらに２ビット精度以上のアナログ・ディジタル変換器１０５を用いることにより、増幅されたノイズ信号１０４の頻度分布を有し、周期性のない乱数データを取得することができる。たとえば、ノイズ源１０１の発生要因が熱雑音であれば、正規分布状の発生確率を有する乱数データを取得することができる。また、アナログ・ディジタル変換されたディジタル値を構成する複数のビットの下位のビットから乱数データを作成すれば、増幅されたノイズ源１

０４の頻度分布形状に依存しない乱数データを取得することができる。

【００７７】更に例えば、１２ビットの精度を有するアナログ・ディジタル変換器を用いて得られた１２ビットの乱数データの中から、下位の２ビットのみを用いると、一様性があり周期性のない２ビットの一様乱数が得られる。

【００７８】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、ランダム事象から起因するノイズ源１０１からノイズ信号１０２を、ＡＣ結合増幅器１０３を用いてアナログ・ディジタル変換器１０５の変換範囲まで増幅してディジタル値に変換して得られたディジタル・データをもとに乱数データを生成するようにしたので、ノイズ源１０１の発生確率分布または一様分布で、周期性がない乱数データを得ることができる。

【００７９】また、本実施形態の物理乱数発生装置では、ノイズ信号のランダム・パルスを計数するのではなく、増幅されたノイズ信号をアナログ・ディジタル変換することにより、１回の変換動作で１つの乱数データを取得することができるため、計数するよりも高速に物理乱数を発生することができる。

【００８０】さらに、２ビット以上の精度を有するアナログ・ディジタル変換器１０５を用いる場合には、１回のアナログ・ディジタル変換で多ビットの乱数データを発生することができ、ひいては回路構成を簡素化することができる。

【００８１】（発明の第２の実施の形態）第１の実施形態では、ランダム・ノイズ源から得られるノイズ信号をアナログ・ディジタル変換器を用いてディジタル・データに変換したときの頻度分布は正規分布となる。この場合、平均値の回りに一様に偶数または奇数データが分布することになり、変換されたディジタル値を構成するすべてのビットの奇数・偶数の頻度分布は一様になる。

【００８２】しかし、増幅回路やアナログ・ディジタル変換器のオフセットの絶対値の存在、またはオフセットのドリフトにより、一様性が崩れる可能性がある。これに対し、本実施形態では、これらをキャンセルするオフセットを加えることにより、奇数・偶数の頻度分布が常に一様になるようにし、一様性が保証された物理乱数を発生するものである。

【００８３】図４は本発明の第２の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図１と同一部分には同一符号を付してその説明を省略する。

【００８４】この物理乱数発生装置は、第１の実施形態と同様に構成される他、アナログ・ディジタル変換器１０５からの出力２０６をもとにオフセット調整信号２０２出力するオフセット検出器２０１と、この信号２０２をＤ／Ａ変換して出力するディジタル・アナログ変換器２０３と、アナログ・オフセット調整信号２０４に変換し、増幅されたノイズ信号１０４から引き去る演算器２０７とを備え、アナログ信号によるオフセット調整機能を有している。

【００８５】次に、以上のように構成された本発明の実施の形態に係る物理乱数発生装置の作用について説明する。

【００８６】第１の実施形態で説明したように、ＡＣ結合増幅器１０３を用いることにより、増幅されたノイズ信号１０４のオフセット成分（直流成分）が小さくなる。しかし、この成分がアナログ・ディジタル変換器１０５自身のオフセット成分と同じ値にならない限り、頻度分布の平均値が０にはならない。すなわちオフセット成分の存在により、アナログ・ディジタル変換器のＭＳＢが０になる確率と１になる確率とが変わるため一様性に誤差が生じるのである。

【００８７】また、微小な他のノイズ成分により正規分布からのずれが発生することも予想される。そこで、正規分布の平均値とアナログ・ディジタル変換器１０５自身のオフセットが一致するよう調整することにより、乱数データの一様性を向上させるのである。

【００８８】また、オフセットや正規分布からのずれが微小であり、温度等の環境条件により変化する可能性もあるため、これらの調整を自動的におこなう必要がある。本実施形態ではこの自動調整方法としてはアナログ方式を採用し、この自動調整機能部分が以下のように動作する。

【００８９】まず、オフセット検出器２０１により、アナログ・ディジタル変換器１０５に変換されたディジタル値２０６からその平均値が求められ、これにより増幅されたノイズ信号１０４とアナログ・ディジタル変換器１０５との間のオフセット量が検出される。

【００９０】オフセット検出器２０１からは検出されたオフセット量に基づきディジタル・オフセット調整信号２０２が出力される。

【００９１】次に、ディジタル・オフセット調整信号２０２がディジタル・アナログ変換器２０３によりＤ／Ａ変換されアナログ・オフセット調整信号２０４として出力される。

【００９２】アナログ・オフセット調整信号２０４は、演算器２０７に入力され、ここで増幅されたノイズ信号１０４から当該調整信号２０４が引き去られ、これによりオフセット量が自動的に零に調整される。

【００９３】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第１の実施形態と同様な構成を設けた他、オフセット検出器２０１、ディジタル・アナログ変換器２０３及び演算器２０７からなるオフセット自動調整機能を設けたので、第１の実施形態と同様な効果が得られる他、増幅回路やアナログ・ディジタル変換器等の種々のオフセットやオフセットドリフト等をキャンセルして奇数・偶数の頻度分布が常に一様になる、一

様性が保証された物理乱数を発生させることができる。

【００９４】（発明の第３の実施の形態）本実施形態では、第２の実施形態と同様なオフセット自動調整機能をディジタル的に実現させるものである。

【００９５】図５は本発明の第３の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図１及び図２と同一部分には同一符号を付してその説明を省略する。

【００９６】この物理乱数発生装置は、第１の実施形態と同様に構成される他、第２の実施形態と同様なオフセット検出器２０１と、オフセット検出器２０１からのディジタル・オフセット調整信号２０２をアナログ・ディジタル変換器１０５からの出力２０６に加算し乱数データとして出力するディジタル加算器２０５を備え、ディジタル信号によるオフセット調整機能を有している。

【００９７】以上のように構成された本発明の実施の形態に係る物理乱数発生装置においては、アナログ信号によるオフセット調整の場合と同様に、オフセット検出器２０１からディジタル・オフセット調整信号２０２が出力される。この調整信号２０２がアナログ・ディジタル変換器１０５からの変換されたディジタル値２０６とディジタル加算器２０５により加算され、オフセット量が自動調整される。

【００９８】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第１の実施形態と同様な構成を設けた他、オフセット検出器２０１及びディジタル加算器２０５からなるオフセット自動調整機能を設けたので、第１及び第２の実施形態と同様な効果が得られる他、第２の実施形態のようにアナログ回路を使用することによる部品点数の増加やオフセット印加回路自身のオフセット電圧変動要素を持ち込みを防止することができる。

【００９９】また、オフセット自動調整機能でもディジタル処理が行われるので、温度特性に依存することもない。さらに、ディジタル回路は容易にＬＳＩ化等の小型化を実現することができ、小形化に際し有利である。

【０１００】（発明の第４の実施の形態）第１の実施形態の物理乱数発生装置において、オフセットの調整をせずにアナログ・ディジタル変換をおこなったとき、増幅器やアナログ・ディジタル変換器のオフセット・ドリフトやゲイン変動、またはノイズ源のノイズ・レベル変動があつた場合、アナログ・ディジタル変換器の上位ビットが特に大きく影響を受けることになる。

【０１０１】シミュレーションによれば、多少のドリフトや変動があった場合でも一様性を保つことができるのは、５ビット目以降のビット・データである。

【０１０２】そこで、本実施形態では、６ビット精度以上のアナログ・ディジタル変換器を使用し、上位から５ビット目以降の２つ以上のビット・データを乱数データとすることにより、各ビットの偶数・奇数発生頻度の一様性を保つ乱数データを発生させるものである。

【０１０３】図６は本発明の第４の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図１と同一部分には同一符号を付してその説明を省略する。

【０１０４】物理乱数発生装置は、第１の実施形態の装置において、アナログ・ディジタル変換器１０５として６ビット精度以上のＡ／Ｄ変換器が使用されるとともに、その変換されたディジタル２０６を構成するビットのうち、上位（ＭＳＢ：Ｍｏｓｔ　Ｓｉｇｎｉｆｉｃａｎｔ　Ｂｉｔ）から５番目以降のビットを乱数データ３０１として取り出すように構成されている。

【０１０５】次に、以上のように構成された本発明の実施の形態に係る物理乱数発生装置の作用について説明する。

【０１０６】図７はオフセット及びゲイン変動に対する一様性に関するシミュレーション結果を示す図である。

【０１０７】まず、図７（ａ）には、オフセットの変動に対する一様性の変化が示めされている。同図に示すように、オフセットをアナログ・ディジタル変換器１０５の変換範囲に対して±１０％程度変化させ、変換されたディジタル値２０６を構成する各ビット毎に、０または１になる頻度を調べると、上位ビットほどオフセットに対する一様性のずれが大きい結果となる。

【０１０８】一方、図７（ｂ）には、ゲインの変動に対する一様性の変化が示めされてる。増幅されたノイズ信号１０４を標準正規分布とし、ゲインを変化させ、アナログ・ディジタル変換器１０５の変換範囲を±６σ～±σとする。このとき、変換されたディジタル値２０６を構成する各ビット毎に、０または１になる頻度を調べると、同図に示すように、上位ビットほどゲイン変動に対する一様性のずれが大きい結果となる。

【０１０９】本実施形態の装置は、以上の知見に基づき、変換されたディジタル値２０６のうち上位から５ビット目以降のデータが乱数データ３０１として取り出される。

【０１１０】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第１の実施形態と同様な構成を設けた他、上位（ＭＳＢ）側から数えて第５ビット以降のビットを乱数データ３０１として採用するようにしたので、第１の実施形態と同様な効果が得られる他、より一層、一様性の良い乱数データを得ることができる。

【０１１１】（発明の第５の実施の形態）本実施形態は、各ビットの偶数・奇数発生頻度の一様性に関するシミュレーション結果に基づき、ノイズ源のノイズ分布に対しアナログ・ディジタル変換器の変換範囲を明確にすることにより、各ビットの偶数・奇数発生頻度の一様性を保つ手法を与えるものである。

【０１１２】図８は本発明の第５の実施の形態に係る物理乱数発生装置におけるＡ／Ｄ変換範囲を決定するためのシミュレーション結果を示す図である。なお、本実施

形態は、図１に示す第１の実施形態と同様な構成を有する物理乱数発生装置に適用される。

【０１１３】図８には、変換されたディジタル値２０６の頻度分布と本実施形態のアナログ・ディジタル変換器の変換値の関係が示されている。同図において、Ｎ±σ以上のアナログ・ディジタル変換器１０５の変換範囲４０１の両側に、オーバーフロー範囲４０２とアンダーフロー範囲４０３が存在しており、これらの範囲４０２及び４０３は、すなわちオーバーレンジ範囲４０４である。

【０１１４】本実施形態の物理乱数発生装置は、このようにアナログ・ディジタル変換器１０５の変換範囲４０１が設定され、第４の実施形態と同様に変換されたディジタル値２０６の５ビット目以降を乱数データに用いる他、第１の実施形態と同様に構成されている。

【０１１５】ここで、ゲインを大きくするということは、頻度分布に対する変換範囲を狭くすることに対応する。ゲインを大きくすると、相対的に平均値付近の変化が少なくなるとみなせるので、オフセットの変動に対する一様性の変化が小さくなり、上位ビットを乱数データとして採用できるようになる。

【０１１６】しかし、増幅されたノイズ信号１０４（図１）がアナログ・ディジタル変換器１０５の変換範囲を越える確率が高くなるため、乱数発生効率が低下する。低下の度合いは、変換されたディジタル値２０６の確率分布に従い、正規分布の場合、アナログ・ディジタル変換器１０５の変換範囲が、増幅されたノイズ信号１０４に対してＮ±σのとき約３０％の損失が生じる。

【０１１７】したがって、変換範囲がＮ±σよりも大きい範囲となるようゲインを下げ、ゲインを下げることによって生じる上位（ＭＳＢ側）ビットの一様性の低下（図７（ｂ）参照）については、変換されたディジタル値２０６の一様性の低下していない５ビット目以降を用いることで対応する。

【０１１８】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第１及び第４の実施形態と同様な構成を設けた他、ノイズ源のノイズ分布に対するアナログ・ディジタル変換器１０５の変換範囲４０１をＮ±σ以上としたので、第１及び第４の実施形態と同様な効果が得られる他、各ビットの偶数・奇数発生頻度の一様性を一層確実に保つことができる。

【０１１９】（発明の第６の実施の形態）本実施形態は、第５の実施形態と同様にアナログ・ディジタル変換器の変換範囲４０１（図８）を予め規定することにより一様性の高い乱数を得ようとするものである。つまり、ノイズ信号がアナログ・ディジタル変換器の変換範囲を越えたときの具体的な取扱いに関する実施形態を示すものである。

【０１２０】変換範囲４０１を越えたときには、アナログ・ディジタル変換器から出力されるディジタル・データの値は保証されない。この場合、変換範囲を越えたときに出力されるデータを構成するビット・パターンが固定化される可能性があり、多ビット・データを乱数データとした時に著しくビット間の相関に影響を与える。

【０１２１】そこで、本実施形態では、変換範囲４０１を越えたときに出力されるデータはランダム性をもたないものとみなし、乱数発生から除外するものである。

【０１２２】図９は本発明の第６の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図１と同一部分には同一符号を付してその説明を省略する。

【０１２３】この物理乱数発生装置は、アナログ・ディジタル変換器１０５からの変換後のディジタル値５０１及びオーバーレンジ信号５０３に基づき、変換範囲４０１内のディジタル値５０１のみを乱数データ１０６として出力するオーバーレンジ処理器５０２が設けられる他、第１の実施形態と同様に構成されている。

【０１２４】このように構成された物理乱数発生装置においては、まず、増幅されたノイズ信号１０４がアナログ・ディジタル変換器１０５の変換範囲を越えた場合には、当該Ａ／Ｄ変換器１０５からオーバーレンジ信号５０３が発生するようになっている。

【０１２５】このオーバーレンジ信号５０３を受けたオーバーレンジ処理器５０２により、アナログ・ディジタル変換後のディジタル値５０１が処理され、オーバーレンジ範囲４０４にあるディジタル値５０１が乱数データ１０６から取り除かれる。ここで、オーバーレンジ処理器５０２の具体的な処理内容は、乱数データ１０６の出力速度により異なることになる。

【０１２６】例えば乱数データ１０６を一定の速度で出力する必要がある場合は、オーバーレンジ処理器５０２にはＦＩＦＯメモリのような緩衝器を内蔵し、オーバーレンジ処理によつて生じるデータ出力の欠落がないように乱数データ１０６が出力される。

【０１２７】この場合、乱数データ出力速度は、アナログ・ディジタル変換器１０５のデータ変換速度より遅くなる。遅くなる割合は、増幅されたノイズ信号１０４をアナログ・ディジタル変換したときの頻度分布で決まる。

【０１２８】乱数データを一定の速度で出力する必要がない場合、たとえば、乱数データ１０６の入出力においてハンドシェイクが行われる場合は、有効な乱数データを得るまでデータ出力を保留する。

【０１２９】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第１の実施形態と同様な構成を設けた他、オーバーレンジ処理器５０２により変換範囲のディジタル値５０１のみを乱数データ１０６として出力するようにしたので、第１の実施形態と同様な効果が得られる他、各ビットの偶数・奇数発生頻度の一様性を一層確実に保つことができる。つまり、変換範囲を越えたときに出力されるデータはランダム性をもたないもの

とみなし、乱数発生から除外することにより、発生した乱数の性質を向上させることができる。

【０１３０】（発明の第７の実施の形態）本実施形態では、アナログ・ディジタル変換器の変換範囲について種々の位置で変換動作を行うことにより、微分非直線性による一様性の低下を改善するものである。

【０１３１】高速なアナログ・ディジタル変換器の微分非直線性は、最悪±０．５ＬＳＢである。たとえば、１０ビット精度のＡ／Ｄ変換器は１．０２４Ｖの電圧を１０２４に分割してデジタル値とすることができるが、微分非直線性の影響により、変換結果がＮとＮ＋１との間の電圧は正確に１ｍＶ（１．０２４／１０２４）にはならない。変換結果Ｎに応じて０．５ｍＶから１．５ｍＶの値となる。これは、アナログ・デジタル変換結果を乱数データとして用いる場合の一様性の低下につながる。

【０１３２】そこで、本発明では、微分非直線性が変換結果Ｎに依存していることを利用し、アナログ信号に既知の電圧を加え、アナログ・ディジタル変換を行ない、アナログ信号に加えた値と同じ値のディジタル値を引き去る機構を物理乱数発生装置に加えるものである。

【０１３３】図１０は本発明の第７の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図である。

【０１３４】この物理乱数発生装置は、アナログ・ディジタル変換器１０５の入力にアナログ補正信号２１０４を加え、変換器１０５の出力からディジタル補正信号２１０２を差し引くように構成される他、第１～第６の実施形態何れかと同様に構成されている。このために物理乱数発生装置には、補正信号発生器２１０１と、ディジタル・アナログ変換器２１０３と、加算器２１０６と、ディジタル減算器２１０５とが設けられている。

【０１３５】このように構成された物理乱数発生装置においては、まず、補正信号発生器２１０１よりディジタル補正信号２１０２が発生する。このディジタル補正信号２１０２は、ディジタル・アナログ変換器２１０３によりアナログ補正信号２１０４に変換され、増幅されたノイズ信号１０４と加算される。この加算値により、アナログ・ディジタル変換器１０５により変換されたディジタル値２０６が得られる。

【０１３６】一方、ディジタル補正信号２１０２は、ディジタル減算器２１０５に入力され、変換されたディジタル値２０６から値を引き去ることにより乱数データ１０６が得られる。

【０１３７】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、アナログ信号に既知の電圧を加え、アナログ・ディジタル変換を行い、アナログ信号に加えた値と同じ値のディジタル値を引き去るようにしたので、第１～第６の実施形態と同様な効果が得られる他、アナログ・ディジタル変換器１０５の変換結果Ｎの値を変えながら、乱数データ１０６としては同じ値を得ることができ、変換結果Ｎに依存した微分非直線性が平均化され、乱数の一様性を改善することができる。

【０１３８】（発明の第８の実施の形態）本実施形態は、第７の実施形態と同様に、アナログ・ディジタル変換器の微分非直線性による一様性の低下を改善するものである。すなわち本実施形態における微分非直線性の影響を低減する基本的な原理は第７の実施形態と同様であり、同じアナログ電圧をディジタル値に変換する場合、異なる値を発生させることにより、変換結果Ｎに依存した一様性の低下を改善するものである。

【０１３９】図１１は本発明の第８の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図である。

【０１４０】この物理乱数発生装置は、アナログ・ディジタル変換器１０５の出力を格納するレジスタ（＃１）２２０１及びレジスタ（＃２）２２０２と、両レジスタ２２０１，２２０１の値を加算するディジタル加算器２２０３が設けられる他、第１～第６の実施形態何れかと同様に構成されている。

【０１４１】このように構成された物理乱数発生装置においては、まず、アナログ・ディジタル変換器１０５により変換されたディジタル値２０６がレジスタ２２０１及びレジスタ２２０２に交互に記録される。

【０１４２】次に、レジスタ２２０１及びレジスタ２２０２の出力のディジタル加算器２２０３により加算平均が求められ、乱数データ１０６として出力される。

【０１４３】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、交互に変換されたディジタル値２０６により加算平均を求めて乱数データ１０６として用いるようにしたので、第１～第６の実施形態と同様な効果が得られる他、変換結果Ｎに依存した乱数一様性の低下を改善し、微分非直線性の影響を低減させることができる。

【０１４４】これにより、アナログ・ディジタル変換されたディジタル値をデータの加算によりビットが１又は０になる確率を一様にすることができる。すなわち加算する相手をランダムな値とすることにより、ランダム性を失うことなく微分非直線性を改善するができる。

【０１４５】なお、図１１に示す構成の物理乱数発生装置では、乱数データ１０６の発生頻度がアナログ・ディジタル変換器１０５の変換頻度の半分になってしまう。

【０１４６】そこで、乱数データ１０６の発生頻度を低下させない方法としては、例えばレジスタ２２０２に入力する値を、もう１系統のノイズ源を用いてディジタル値に変換された値を用いてもよい。また、乱数データとして多ビットを用いるのでなければ、周期的なディジタル値をレジスタ＃２に接続して加算（排他ＯＲ）することによつて、一様性を向上することもできる。

【０１４７】（発明の第９の実施の形態）本実施形態で

は、上記第１～第８の実施形態に使用され得るノイズ源として、アナログ・ディジタル変換した場合の頻度分布が正規分布に従うノイズ源について説明する。本実施形態は熱雑音を利用するものであり、熱雑音は統計的事象から引き起こされ、熱雑音のゆらぎは正規分布になる。

【０１４８】図１２は本発明の第９の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源１０１は、第１～第８の実施形態に示す物理乱数発生装置に適用されるものである。

【０１４９】このノイズ源１０１は抵抗の熱雑音を利用するものであり、ノイズ源１０１においては電源Ｖから抵抗６０１と抵抗６０２とが直列接続され接地され、同様にた電源Ｖからヒータ６０３とヒータ６０４とが直列接続され接地されている。また、このヒータ６０３及びヒータ６０４は、それぞれ抵抗６０１及び抵抗６０２を加熱するように配置され、抵抗６０１と抵抗６０２との間からノイズ信号１０２が出力されるようになっている。

【０１５０】抵抗の熱雑音は小さいため、ヒータ６０３およびヒータ６０４により抵抗を加熱し、熱雑音を大きくするとともに、抵抗６０１および抵抗６０２の温度を一定とすることにより、安定したノイズ信号１０２が得られる。

【０１５１】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【０１５２】（発明の第１０の実施の形態）本実施形態では、第９の実施形態と同様に、上記第１～第８の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【０１５３】図１３は本発明の第１０の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源１０１は、第１～第８の実施形態に示す物理乱数発生装置に適用されるものである。

【０１５４】このノイズ源１０１は、トランジスタを使用するものであり、電源接地間に直列接続された抵抗７０１及び抵抗７０２との間からトランジスタ７０３に接続している。これによりトランジスタ７０３にバイアスが掛けられる一方、電源接地間に抵抗７０４、トランジスタ７０３及び抵抗７０７が直列接続されている。そして、抵抗７０４の両端に発生するトランジスタ７０３の熱雑音を利用し、抵抗７０４、トランジスタ７０３間からノイズ信号１０２が出力されるようになっている。

【０１５５】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【０１５６】（発明の第１１の実施の形態）本実施形態では、第９の実施形態と同様に、上記第１～第８の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【０１５７】図１４は本発明の第１１の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源１０１は、第１～第８の実施形態に示す物理乱数発生装置に適用されるものである。

【０１５８】このノイズ源１０１は、ツェナーダイオードを使用する場合であり、電源接地間に抵抗７０５とツェナーダイオード７０６が接続され、この両者間からノイズ信号１０２が出力されるようになっている。

【０１５９】このようにツェナーダイオードを用いる場合には、抵抗７０５によりツェナーダイオード７０６にツェナー電流を流し、抵抗７０５の両端に発生する熱雑音を利用する。ツェナーダイオード７０６に電流を流す回路としては、抵抗ではなく例えば定電流回路でも良い。

【０１６０】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【０１６１】（発明の第１２の実施の形態）本実施形態では、第９の実施形態と同様に、上記第１～第８の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【０１６２】図１５は本発明の第１２の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源１０１は、第１～第８の実施形態に示す物理乱数発生装置に適用されるものである。

【０１６３】このノイズ源１０１は、フォトマルチプライヤを利用するものであり、同図に示すように、フォトマルチプライヤ８０１、バイアス印加用の抵抗８０６，８０７及び８０８並びに高圧電源８０９より構成される。

【０１６４】フォトマルチプライヤ８０１は、光を電子に変換して増幅する。

【０１６５】すなわちフォトマルチプライヤ８０１の光電面８０２に光が当たると、そこから電子が発生する。発生した電子は電位の高い電極８０３に衝突し、電極８０３への電子衝突によりさらに多数の電子が発生する。この発生した電子は、さらに電位の高い電極８０４に衝突する。

【０１６６】このような電子の増倍を繰り返し、最後の電極８０５に電子が衝突する。ここまでに到達した電子

の数から光電面に入射した非常に微弱な光の量を知ることができ、ここよりノイズ信号１０２が得られる。

【０１６７】ところで、光電面８０２を遮光した場合でも、光電面に存在する熱電子によりフォトマルチプライヤの出力にはノイズ信号１０２が発生する。通常、このようにして発生するノイズを暗電流と呼び、光の量を測定するときの下限となるため小さい方が良いとされるが、熱雑音に起因したノイズであるため物理乱数のノイズ源として利用できる。

【０１６８】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【０１６９】（発明の第１３の実施の形態）本実施形態では、第９の実施形態と同様に、上記第１～第８の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【０１７０】図１６は本発明の第１３の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源１０１は、第１～第８の実施形態に示す物理乱数発生装置に適用されるものである。

【０１７１】このノイズ源１０１は、真空管を利用するものであり、高圧電源９０６がバイアス印加用の抵抗９０５を介して２極真空管９０１に接続され、この２極真空管９０１にはさらにヒータ電源９０７が接続されて構成されている。

【０１７２】２極真空管９０１においては、ヒータ９０２を用いて電極９０３を加熱することにより熱電子が発生し、発生した電子は電位の高い電極９０４に到達する。電極９０３から電極９０４に流れた電子の量は、抵抗９０５の両端電圧を測定することにより得られる。

【０１７３】得られた電流値は、熱雑音を起因とするゆらぎを有し、このゆらぎをノイズ信号１０２として使用する。なお、ここで使用するヒータ電源９０７にはＡＣノイズの影響が出ないよう直流電源を用いることが望ましい。

【０１７４】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【０１７５】（発明の第１４の実施の形態）本実施形態では、第９の実施形態と同様に、上記第１～第８の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【０１７６】図１７は本発明の第１４の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源１０１は、第１～第８の実施形態に示す物理乱数発生装置に適用されるものである。

【０１７７】このノイズ源１０１は、真空マイクロ素子を利用するものであり、高圧電源１００６がバイアス印加用の抵抗１００５を介して真空マイクロ素子１００１に接続され、この真空マイクロ素子１００１には制御電源１００７が接続されて構成されている。

【０１７８】接地された電極１００２の近傍に電極１００３をおき、この電極１００３に制御電源１００７より電場をかけると、トンネル効果により電極１００２から電子が発生する。発生した電子は電極１００３に向って移動するが、電極１００２とで電極１００３を挟むように配置される，より高い電位の電極１００４に引きつけられる。このようにして、電極１００２と電極１００４との間に電流が流れ、流れた電流は抵抗１００５の両端電圧として観測される。得られた電流値は統計的に発生するトンネル効果を起因とするゆらぎを有し、このゆらぎをノイズ信号１０２として使用する。

【０１７９】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【０１８０】（発明の第１５の実施の形態）本実施形態は、第９～第１３の実施形態のノイズ源に適用されるものであって、ノイズ源からのノイズ信号を安定化させるためのものである。

【０１８１】すなわち、熱雑音は絶対温度の平方根に比例して変動することから、ノイズ源から発生する信号レベルが周囲温度の影響により変動するので、これを防止するものである。

【０１８２】なお、第１４の実施形態に示す真空マイクロ素子のゆらぎ成分は、トンネル効果によるものであり、温度の影響を受けないためこの方法による定温化の効果が得られないことから除外している。

【０１８３】図１８は本発明の第１５の実施の形態に係る物理乱数発生装置におけるノイズ源恒温化装置の一例を示す構成図である。

【０１８４】このノイズ源恒温化装置では、ノイズ源素子２００１を恒温ケース２００２に収納する。恒温ケース２００２には、ヒータ２００３が内蔵されており、恒温制御器２００５により温度が一定になるよう制御されている。なお、ノイズ源素子２００１は、第７～第１２の実施形態のノイズ源１０１に使用されるノイズ源の素子部分である。

【０１８５】ノイズ源素子２００１の温度は、測温体２００４を用いて測定し、温度信号２００６として恒温制御器２００５に接続される。恒温制御器２００５は、温度信号２００６にもとづきヒータ加熱信号２００７を制御し、ノイズ源素子２００１の温度が一定になるようヒ

ータ加熱電力を制御する。

【０１８６】一定に制御する温度としては、ノイズ源素子２００１の動作限界よりも低く、環境温度よりも高い温度を選択する。たとえば、コンピュータ周囲温度を２５℃、物理乱数発生装置の周辺温度を３５℃、ノイズ源素子２００１の上限動作温度を５５℃とし、コンピュータ周辺温度が空調により±５℃変化して物理乱数発生装置の周辺温度が最高４０℃まで上昇すると仮定した場合、制御する温度の値を４５℃～５０℃にすれば、冷却機能を内蔵せずにノイズ源素子２００１の温度をヒータ２００３だけで一定に制御することができる。

【０１８７】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、そのノイズ源１０１をノイズ源恒温化装置により温度を一定に保つようにしたので、ノイズレベルの変動を防ぐとともに、高温で一定に保つことにより、熱雑音が出やすくなり、さらに冷却を不要とすることができる。

【０１８８】（発明の第１６の実施の形態）本実施形態から第２３の実施形態までは第１～第１５の実施形態で説明した物理乱数発生装置を利用した装置について説明する。

【０１８９】図１９は本発明の第１６の実施の形態に係る物理乱数発生装置を用いた表示装置の構成例を示すブロック図である。

【０１９０】この表示装置は、物理乱数発生回路１００からの乱数データ１０６が表示処理器１１０１に入力され、さらにこの表示処理器１１０１からの表示データ１１０２が表示器１１０３に表示されるようになっている。

【０１９１】表示処理器１１０１は、制御パネル１１０４の制御により、入力された乱数データ１０６を利用して入力し表示データ１１０２を出力する。

【０１９２】制御パネル１１０４には、ボタン等が付いており、ボタンを押した結果が制御信号１１０５として表示処理器１１０１に入力されるようになっている。

【０１９３】物理乱数発生回路１００は、第１～第１５の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【０１９４】なお、この物理乱数発生回路１００及び表示処理器１１０１からなる乱数出力部分には、種々の乱数発生機能が組み込まれている。この種々の乱数発生機能は、例えばアナログ・ディジタル変換器１０５のビット数を変更することで発生させる一様乱数データ１０６の値の範囲を変更し、表示処理器１１０１にて受信した乱数データ１０６の取捨選択をするものである。

【０１９５】このように構成された物理乱数発生装置を用いた表示装置の動作について説明する。

【０１９６】たとえば、サイコロの目を乱数で出す場合を考える。まず、制御パネル１１０４のボタンで乱数発生機能をサイコロモードに切り替える。

【０１９７】ここで３ビットの一様乱数データ１０６を用いて０から７の値を発生するが、サイコロには１から６の目しかないので、０または７が出たときは、１から６の目が出るまで乱数を発生するようにしておく。

【０１９８】制御パネル１１０４のボタンを押して乱数の発生を開始する。乱数の発生を開始したことが分かるように発生した乱数の値を表示器１１０３に表示する。次にボタンを押して乱数の発生を停止し、そのときの乱数の値を表示器１１０３に表示する。

【０１９９】次に、ビンゴゲームの数字を出す場合を考える。まず、制御パネル１１０４のボタンで乱数発生機能をビンゴモードに切り替える。発生させた乱数データのうち、ビンゴゲームに必要のない数値が出たときの処理はサイコロのときと同じであるが、ビンゴゲームの場合は値は１度しか発生しないため、１度発生した値を覚えておく必要がある。さらに、ゲームが終了したら、１度発生した値をすべて消去する機能も必要であるから、ビンゴモードのスタート、ストップ機能のボタンに加えてリセット機能を有するボタンも必要である。

【０２００】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた表示装置においては、物理乱数発生回路１００、表示処理器１１０１及び制御パネル１１０４を設けたので、手軽に乱数を取得し、種々の用途に応用することができる。たとえば乱数表の作成、さいころの模擬、ビンゴゲームの数字発生、福引き抽選機等の用途に使用できる。このような用途に適用することで、ノイズ源および乱数データ発生回路の大量生産が可能になり、装置の小型化、低価格化を実現させることができる。

【０２０１】（発明の第１７の実施の形態）本実施形態では、物理乱数発生装置を用いた通信装置について説明する。このような通信方法として例えばスペクトラム拡散方式があり、物理乱数発生装置で発生した乱数データを用いて周波数変調を行なうことにより、第三者に知られることなく通信することができる。このような用途の乱数には、乱数に周期性がないことと、一様性が求められる。疑似乱数は周期性があり一様性も完全ではないので、乱数としては物理乱数を用いるほうが適している。

【０２０２】図２０は本発明の第１７の実施の形態に係る物理乱数発生装置を用いた通信装置の構成例を示すブロック図である。

【０２０３】この通信装置は、物理乱数発生回路１００、変調信号発生器１２０１及び変調器１２０３により構成されている。なお、物理乱数発生回路１００は、第１～第１５の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【０２０４】このように構成された物理乱数発生装置を用いた通信装置は以下のように動作する。

【０２０５】まず、物理乱数発生回路１００からの乱数データ１０６をもとに変調信号発生器１２０１におい

て、変調信号１２０２が生成される。そして、送信データ１２０４と変調信号１２０２が変調器１２０３により変調され、送信信号１２０５が作成され送信される。

【０２０６】スペクトラム拡散方式の通信方式では、このように乱数データから変調信号を作成している。データ通信の場合は、第３者に変調信号を知られてはならないが、通信をおこなう者同士は変調信号を互いに知っておく必要がある。

【０２０７】そこで、変調信号発生器１２０１の役割は、乱数データ１０６から変調信号を作成し、新たな変調信号を通信を行う者同士で認識されるまで保持し、認識された時点で新しい変調信号に更新することにある。

【０２０８】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた表示装置においては、スペクトラム拡散方式の通信等に物理乱数発生回路１００からの物理乱数データ１０６を使用するようにしたので、装置の小型化、低価格化を実現させることができるとともに、通信の秘匿性を確実に確保することができる。

【０２０９】すなわち疑似乱数のように、一定のルールで作成された変調信号の場合、一旦変調信号を解読すると新たな変調信号を発生しても容易に推定されるという問題があるが、物理乱数の場合は周期性や発生する順番に関するルールがないため、一度解読されても容易に類推することができない。

【０２１０】（発明の第１８の実施の形態）本実施形態では、物理乱数発生器を用いたデータ暗号化装置について説明する。たとえば、ＡＢＣという文字を暗号化して他の３文字に置き換えるために乱数データを用いる。また、戦闘機において、互いに見方であることを示す識別コードとして暗号が使用されている。このような暗号は頻繁に変更し、第３者に容易に解読されない必要がある。

【０２１１】図２１は本発明の第１８の実施の形態に係る物理乱数発生装置を用いたデータ暗号化装置の構成例を示すブロック図である。

【０２１２】このデータ暗号化装置は、物理乱数発生回路１００、暗号化装置１３０２により構成されている。なお、物理乱数発生回路１００は、第１～第１５の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【０２１３】このように構成された物理乱数発生装置を用いたデータ暗号化装置は以下のように動作する。

【０２１４】元データ１３０１とともに物理乱数発生回路１００からの乱数データ１０６が暗号化装置１３０２に入力される。暗号化装置１３０２においては、この元データ１３０１及び乱数データ１０６によって、暗号化データ１３０３が作成され出力される。

【０２１５】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた表示装置においては、暗号化に物理乱数発生回路１００からの乱数データ１０６を利用するようにしたので、装置の小型化、低価格化を実現させることができるとともに、暗号化するコードとして物理乱数データ１０６を使用することにより、周期性、データ発生の順番などの問題をなくすことができ、暗号化の秘匿性を向上させることができる。

【０２１６】なお、従来のように、この乱数として疑似乱数を使用する場合、周期性や一様性に関する課題がある。すなわち良く知られている疑似乱数発生手法を用いて発生された乱数データについては、研究され尽くされており、乱数系列の一部から乱数系列全体を推定することも可能になっているため、疑似乱数では完全な秘匿性を確保できない可能性がある。これに対し、物理乱数発生装置から得られる乱数データは、周期性がなく、一様性が保証された良質の乱数であるため、秘匿性を確保することができる。

【０２１７】（発明の第１９の実施の形態）本実施形態では、発生した物理乱数データを計算機に取り込むことを可能にする乱数入力装置について説明する。

【０２１８】図２２は本発明の第１９の実施の形態に係る物理乱数発生装置を用いた乱数入力装置の一構成例を示すブロック図である。

【０２１９】図２３は本発明の第１９の実施の形態に係る物理乱数発生装置を用いた乱数入力装置の他の構成例を示すブロック図である。

【０２２０】図２４は本発明の第１９の実施の形態に係る物理乱数発生装置を用いた乱数入力装置のさらに他の構成例を示すブロック図であり、図１９～図２１において同一部分には同一符号を付している。

【０２２１】図２２～図２４に示す乱数入力装置においては、物理算数発生回路１００から出力された乱数データ１０６がバス・インタフェース１４０１に入力され、さらにバス・インタフェース１４０１からバスインタフェース信号１４０２に変換された乱数が計算機に対して出力されるようになっている。

【０２２２】なお、物理乱数発生回路１００は、第１～第１５の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【０２２３】バスインタフェース信号１４０２は、コンピュータ・データ入出力バス１４０３（図２２，図２３）あるいはカード内部バス１４０４（図２４）を介して計算機内に入力されるが、この部分及び全体のパッケージ等は図２２～図２４に示す乱数入力装置毎に異なっている。なお、図２２，図２３の装置において、バス・インタフェース１４０１は、コンピュータ・データ入出力バス１４０３を介して受け取った計算機からの命令に基づき、物理乱数発生回路１００から乱数データ１０６を取得し、要求元の計算機に送信する。

【０２２４】図２２の場合は、乱数入力装置が基板として提供される例である。この基板形態では、物理乱数発生基板１４００ａをＰＣＩバスのようなコンピュータの

スロットに挿入して使用される。

【０２２５】図２３の場合は、乱数入力装置がカードとして提供される例である。このカード形態では、物理乱数発生カード１４００ｂをＰＣＭＣＩＡのようなカード用のスロットに挿入して使用される。

【０２２６】図２４の場合は、乱数入力装置がＩＣカード１４００ｃとして提供される例である。なお、ＩＣカードはＣＰＵ（図示せず）が内蔵され一種の計算機であるとみなせるので、この場合は乱数入力装置が計算機自体に組み込まれた形になっている。

【０２２７】すなわちＩＣカード１４００ｃにはＣＰＵが内蔵されているため（図示せず）、コンピュータ・データ入出力バス１４０３ではなく、カード内部バス１４０４を経由してＩＣカード内部のＣＰＵへ乱数データを出力することになる。このような形態にすることにより、セキュリティ上性質の良い乱数が必要なＩＣカードを実現することができる。

【０２２８】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた乱数入力装置においては、計算機への乱数入力に物理乱数発生回路１００からの乱数データ１０６を利用するようにしたので、装置の小型化、低価格化を実現させることができる。

【０２２９】また特に、コンピュータの入出力バスとして、ＰＣＩバスのような汎用性のあるバスを用いれば、１品種の基板の開発により、パソコンのような小さな計算機からＥＷＳや並列計算機まで対応することができるようになり、大量生産が可能になる。これにより本発明の目的である低価格化がより効果的に実現される。

【０２３０】（発明の第２０の実施の形態）本実施形態では、１個の物理乱数発生装置をネットワークに接続して、複数の計算機に乱数データを供給することを可能にする。

【０２３１】図２５は本発明の第２０の実施の形態に係る物理乱数発生装置の構成例を示すブロック図である。

【０２３２】この物理乱数発生装置は、物理乱数発生回路１００及びネートワーク・インターフェイス１５０１から構成されている。なお、物理乱数発生回路１００は、第１～第１５の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【０２３３】ネットワーク・インターフェイス１５０１は、ネートワーク・ケーブル１５０２を介して受け取った命令にもとづき、物理乱数発生回路１００から乱数データ１０６を取得し、ネットワークに送信する。

【０２３４】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、ネットワークに提供する乱数に、物理乱数発生回路１００からの乱数データ１０６を利用するようにしたので、安価に複数の計算機において物理乱数を利用することができる。

【０２３５】すなわち、１台の専用物理乱数発生装置から複数の計算機にデータを供給するため、計算機１台あたり物理乱数発生に関わる単価を低く抑えることができる。そのため、本発明の目的である低価格化を実現することができる。

【０２３６】（発明の第２１の実施の形態）本実施形態では、物理乱数データの要求に対する供給を安定化する記録再生機能付きの物理乱数発生装置について説明する。

【０２３７】特に、乱数データを要求する相手が計算機の場合、乱数データだけを高速に要求する可能性は小さく、乱数データの要求を行う間にいくつかの演算を行うため、物理乱数発生装置の乱数データ供給が過剰になることが多い。

【０２３８】そこで、本実施形態の物理乱数発生装置は、たとえば物理乱数データの要求が少ない夜間に乱数データを記憶装置に記録しておき、要求に対する乱数データの供給を記憶装置から行うことにより、記憶装置の容量までの要求に対して充分に高速に乱数データの提供を可能とするものである。

【０２３９】図２６は本発明の第２１の実施の形態に係る物理乱数発生装置の構成例を示すブロック図である。

【０２４０】この記録再生機能付きの物理乱数発生装置は、物理乱数発生回路１００、記憶装置インターフェイス１６０１及び記憶装置１６０４より構成されている。なお、物理乱数発生回路１００は、第１～第１５の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【０２４１】記憶装置インターフェイス１６０１は、乱数データ１０６を一旦記憶装置１６０４に記録し、図示しない外部装置の要求に従って、記憶装置１６０４から乱数データを再生して再生乱数データ１６０５として出力する。

【０２４２】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、乱数の出力頻度にばらつきがあるような状態で乱数データ１０６を使用する場合、緩衝の役割をする記憶装置１６０４を用いることにより、乱数発生の要求が瞬間的に多くなっても対応することができる。

【０２４３】すなわち過剰に発生した乱数データを、一旦記憶装置に記録することにより、瞬間的に乱数データの要求が発生する場合の緩衝が可能になり、安定に乱数データを供給することができる。

【０２４４】（発明の第２２の実施の形態）本実施形態では、物理乱数データをフロッピ・ディスクやＣＤ－ＲＯＭのような記憶媒体に記録して提供することを可能とする物理乱数発生装置について説明する。

【０２４５】物理乱数は、周期性のない一様な質の良い乱数を発生することができる反面、発生する乱数データの順序を予測できないことが利用上の課題となることがある。たとえば、送信するデータを暗号化する場合、受信側が持っている媒体に記録された内容と同じ内容を記

録した媒体を利用し、送信データと一緒に暗号化に使用した乱数データが存在する場所だけを示すデータ（解読キー）を送信することにより、第三者に全く解読されない状態で情報のやり取りができるようになる。そこで、本実施形態では第１～第１５の実施形態の物理乱数発生装置の何れかで作成した物理乱数データを可搬な媒体に記録する。このための記録媒体としては、ＦＤ、ＭＯ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等が用いられる。

【０２４６】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、第１～第１５の実施形態の物理乱数発生装置で生成した物理乱数データを可搬な媒体に記録するようにしたので、物理乱数データを記録した媒体を通信を行う当事者間で保有することができ、第３者に知られることなくデータの暗号化／解読を行なうことができる。

【０２４７】これにより、ハードウエアを購入するよりもはるかに安価に乱数データを取得することができる。

【０２４８】（発明の第２３の実施の形態）本実施形態では、第２２の実施形態において乱数データの質を保証して供給するようにしたものである。

【０２４９】乱数の質を示すための検定手法は複数あり、乱数を使用する場合はいくつかの検定を行った上で乱数データを利用するのが一般的であるが、そのためのソフトウエア開発等の作業に要する時間は膨大になる。したがって、本実施形態では乱数の質を示す検定方法と検定結果を乱数データとともに記録した可搬な媒体を供給するようにしたものである。

【０２５０】本実施形態では第１～第１５の実施形態の物理乱数発生装置の何れかで作成した物理乱数データを可搬な媒体に記録するとともに、当該媒体にその検定方法及び検定結果を記録する。

【０２５１】ここで、検定方法について説明する。

【０２５２】与えられた数列を乱数列と見なして良いか否かを判定するための確固たる手順は、現在のところ存在しないといってもよい。普通に使われている方法は、その数列が、一様母集団からのランダムサンプルであるという仮設を、幾つかの方法で検定し、その総合結果から判断する，というものである。

【０２５３】検定の種類とか、実行手順、パラメータの選択等については、検定を行う者の好みにまかされており、標準的な検定方法さえ確立していない。

【０２５４】検定方法には以下のようなものがある。

【０２５５】まず、

（１）一次元、二次元、三次元の頻度検定

（２）マルコフ性の検定

与えられた数列を、状態間の推移が等確率であるようなマルコフ過程の一つの実現値と見て、標本推移度数の等確率性を検定する。

【０２５６】

（３）モーメント（平均、分散）の検定

（４）遅れが１，２，．．．の系列相関係数の検定

（５）二次元、三次元のランダム距離の検定

（６）連の検定（上昇連、下降連の長さの分布、個数の平均、符号連）

等が考えられる。

【０２５７】また、他の方法（日本規格協会等の乱数表の検定に用いられている伝統的な方法）として、

（１）一次元度数検定

（２）二次元度数検定（系列検定）

（３）ポーカー検定

（４）連の検定（上昇連、下降連）

（５）ギャップの検定

（６）衝突検定

（７）ＯＰＳＯ検定

等も考えられる。

【０２５８】さらに、他の方法（パチンコ台用の乱数発生器）として、

（１）一次元度数検定

（２）二次元度数検定

（３）スペクトル検定

（４）相関係数による検定

（５）自己相関係数、偏自己相関係数による検定

（６）連の検定

等も考えられる。

【０２５９】また、このための媒体としては、ＦＤ、ＭＯ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等が用いられる。

【０２６０】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、第１～第１５の実施形態の物理乱数発生装置で生成した物理乱数データ、その検定方法及び検定結果を可搬な媒体に記録するようにしたので、第２２の実施形態と同様な効果が得られる他、その検定方法及び検定結果により、媒体に記録された乱数データの質を容易に確認することができる。

【０２６１】すなわち媒体に記録された乱数データを利用するユーザが改めて検定を行うことなく安心してデータを利用することができ、物理乱数の普及につながるものである。

【０２６２】なお、上記各実施形態の物理乱数発生装置により得られる効果を整理すると以下の通りである。

【０２６３】（１）物理乱数発生速度の向上

従来の乱数発生方法が、ランダム・パルスの計数によるものであったのに対し、本発明ではノイズ源を直接サンプリングして得られる統計的分布を利用したものであるため、乱数を高速に発生することができる。

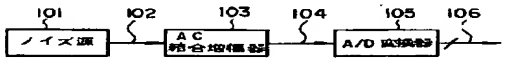
【０２６４】（２）ノイズ源および乱数発生処理回路の簡素化

従来の乱数発生方法では、１つのノイズ源に対して１ビットの乱数発生であったのに対し、本発明ではアナログ・ディジタル変換器を用いることにより、１度に複数のビットを発生することができる。

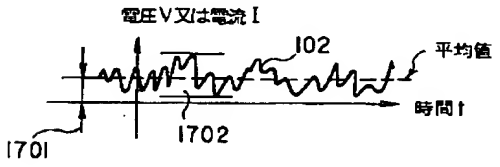
【０２６５】（３）乱数として良質な特性を有する乱数の提供
熱雑音のような統計的現象を電気的にとらえているので、発生する乱数は自然界のランダム現象に基づくものであり、良質な特性を有する乱数の提供が可能である。
【０２６６】（４）乱数発生装置の幅広い分野への適用
計算機への応用ではパソコンから汎用コンピュータ、民生用ではゲーム機やパチンコ台、そしてＩＣカードへの適用を行うことができる。
【０２６７】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。
【０２６８】また、実施形態に記載した手法は、計算機に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。
【０２６９】
【発明の効果】以上詳記したように本発明によれば、物理乱数発生速度を向上するとともに、乱数として良質な特性を有する物理乱数を提供し、汎用のコンピュータからパソコンやゲーム機のような民生レベルまで幅広い分野への適用をできるようにした物理乱数発生装置及び方法、物理乱数入力装置並びに物理乱数記録媒体を提供することができる。
【図面の簡単な説明】
【図１】本発明の第１の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【図２】同実施形態の物理乱数発生装置におけるＡＣ結合増幅器の内部構成例を示す図。
【図３】ノイズ信号波形の例を示す図。
【図４】本発明の第２の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【図５】本発明の第３の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【図６】本発明の第４の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【図７】オフセット及びゲイン変動に対する一様性に関するシミュレーション結果を示す図。
【図８】本発明の第５の実施の形態に係る物理乱数発生装置におけるＡ／Ｄ変換範囲を決定するためのシミュレーション結果を示す図。
【図９】本発明の第６の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【図１０】本発明の第７の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図。
【図１１】本発明の第８の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図。
【図１２】本発明の第９の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。
【図１３】本発明の第１０の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。
【図１４】本発明の第１１の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。
【図１５】本発明の第１２の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。
【図１６】本発明の第１３の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。
【図１７】本発明の第１４の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。
【図１８】本発明の第１５の実施の形態に係る物理乱数発生装置におけるノイズ源恒温化装置の一例を示す構成図。
【図１９】本発明の第１６の実施の形態に係る物理乱数発生装置を用いた表示装置の構成例を示すブロック図。
【図２０】本発明の第１７の実施の形態に係る物理乱数発生装置を用いた通信装置の構成例を示すブロック図。
【図２１】本発明の第１８の実施の形態に係る物理乱数発生装置を用いたデータ暗号化装置の構成例を示すブロック図。
【図２２】本発明の第１９の実施の形態に係る物理乱数発生装置を用いた乱数入力装置の一構成例を示すブロック図。
【図２３】同実施形態の物理乱数発生装置を用いた乱数入力装置の他の構成例を示すブロック図。
【図２４】同実施形態の物理乱数発生装置を用いた乱数入力装置のさらに他の構成例を示すブロック図。
【図２５】本発明の第２０の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【図２６】本発明の第２１の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。
【符号の説明】
１０１…ノイズ源
１０３…ＡＣ結合増幅器
１０５…アナログ・ディジタル変換器
１０６…乱数データ
２０１…オフセット検出器
２０３…ディジタル・アナログ変換器
２０５…ディジタル加算器
４０１…アナログ・ディジタル変換器の変換範囲
４０２…オーバーフロー範囲

４０３…アンダーフロー範囲
４０４…オーバーレンジ範囲
５０２…オーバーレンジ処理器
６０１，６０２…抵抗
６０３，６０４…ヒータ
７０１，７０２，７０４，７０５，７０７…抵抗
７０３…トランジスタ
７０６…ツェナーダイオード
８０１…フォトマルチプライヤ
８０６，８０７，８０８…バイアス印加用の抵抗
８０９…高圧電源
９０１…２極真空管
９０５…バイアス印加用の抵抗
９０６…高圧電源
９０７…ヒータ電源
１００１…真空マイクロ素子
１００５…バイアス印加用の抵抗
１００６…高圧電源
１００７…制御電源
１１０１…表示処理器
１１０３…表示器
１１０４…制御パネル
１２０１…変調信号発生器
１２０３…変調器
１３０２…暗号化装置
１４０１…バス・インタフェース
１４０３…コンピュータ・データ入出力バス
１４０４…カード内部バス
１５０１…ネートワーク・インターフェイス
１５０２…ネートワーク・ケーブル
１６０１…記憶装置インターフェイス
１６０２…記憶装置
１８０１…入力コンデンサ
１８０２…増幅器
１８０３…出力コンデンサ
２００１…ノイズ源素子
２００２…恒温ケース
２００３…ヒータ
２００５…恒温制御器
２１０１…補正信号発生器
２１０３…ディジタル・アナログ変換器
２１０５…ディジタル減算器
２１０６…加算器
２２０１…レジスタ
２２０２…レジスタ
２２０３…ディジタル加算器

【図１】

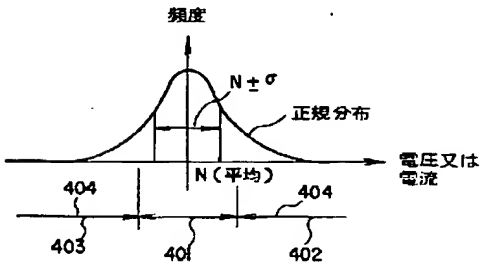


【図３】



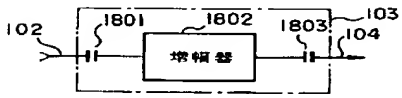
ノイズ信号波形の例

【図８】

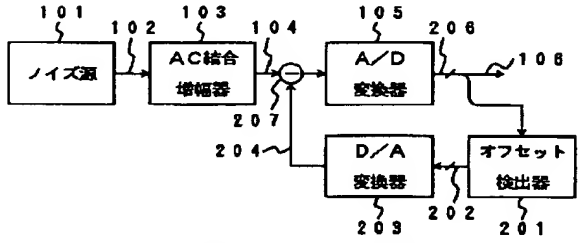


ディジタル値の頻度分布とＡＤＣの変換範囲

【図２】

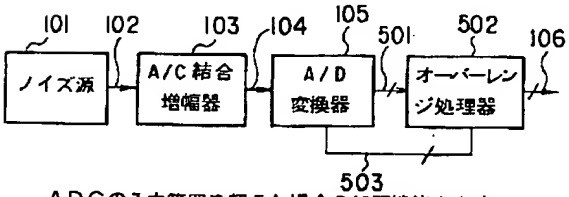


【図４】



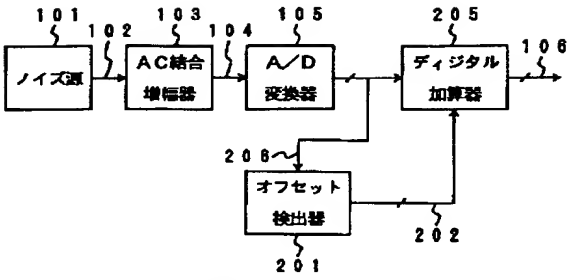
アナログ信号によるオフセット調整

【図９】



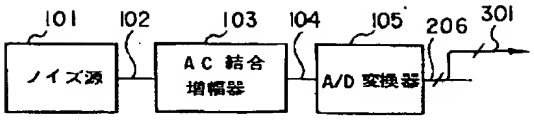
ＡＤＣの入力範囲を超えた場合の処理機能を有する物理乱数発生装置の構成例

【図５】



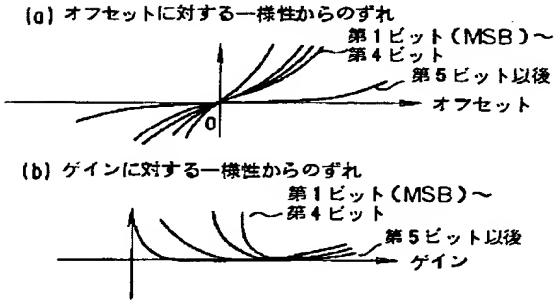
ディジタル値によるオフセット調整

【図６】



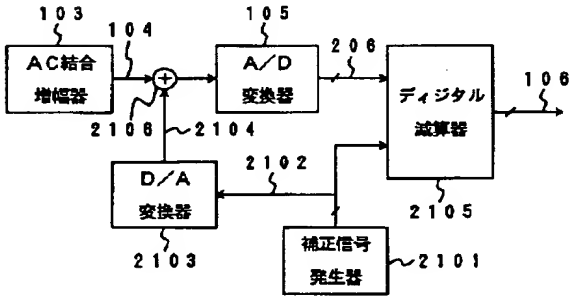
アナログ・ディジタル変換されたディジタル値の
うち　上位から５ビット目以降の２つ以上の
ビットデータを取り出す構成例

【図７】



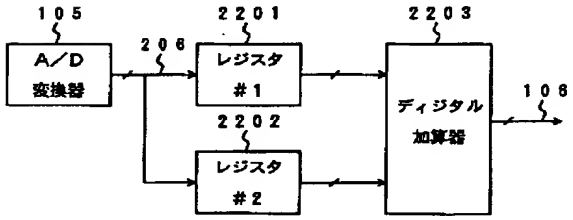
オフセットおよびゲイン変動に対する一様性

【図１０】



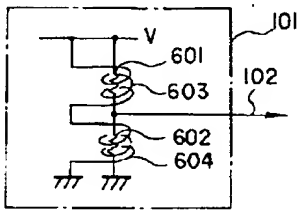
微分非直線性を改善した物乱数発生装置の構成例

【図１１】



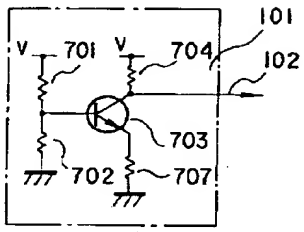
加算平均化により微分非直線性の影響を改善した
物理乱数発生装置の構成例

【図１２】



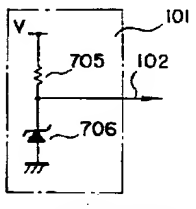
抵抗の熱雑音をノイズ源とする場合の構成例

【図１３】



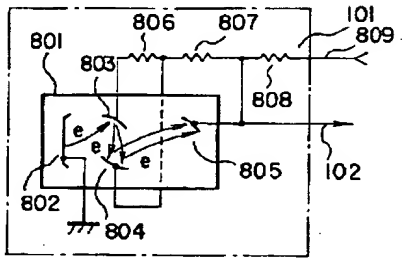
トランジスタを使用する場合

【図１４】



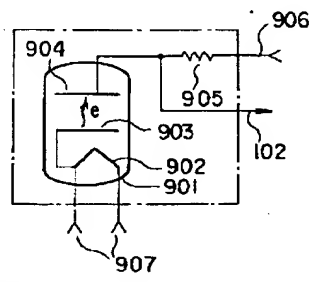
ダイオードを使用する場合

【図１５】



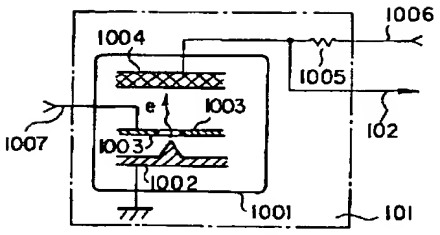
フォトマルチプライヤをノイズ源とする場合の構成例

【図１６】



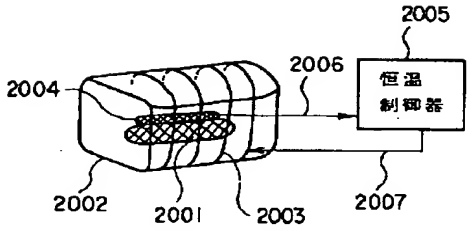
真空管をノイズ源とする場合の構成例

【図１７】



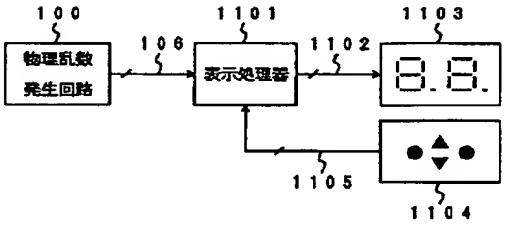
真空マイクロ素子をノイズ源とする場合の構成例

【図１８】



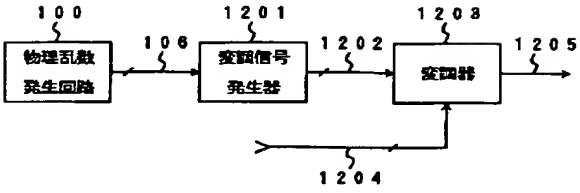
ノイズ源の恒温化の例

【図１９】



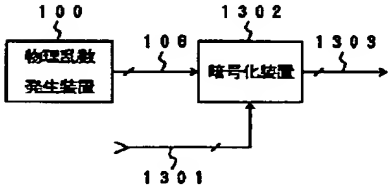
乱数データの表示機能付物理乱数発生装置の構成例

【図２０】



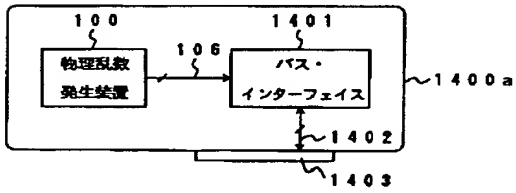
乱数データによる変調機能付物理乱数発生装置の構成例

【図２１】



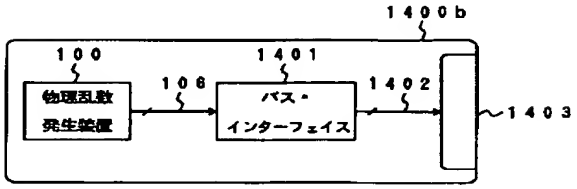
乱数データによる暗合化機能付物理乱数発生装置の構成例

【図２２】



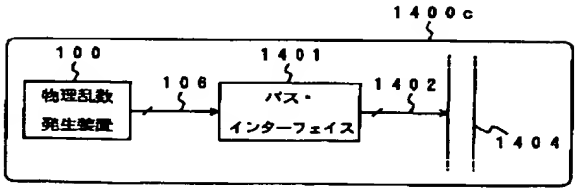
基板形態の例

【図２３】



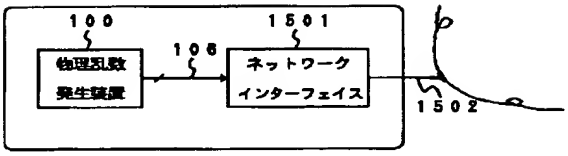
カード形態の例

【図２４】



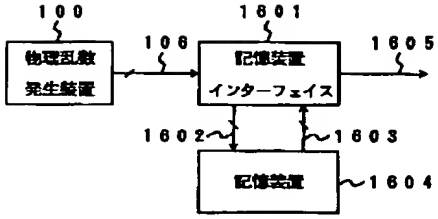
ＩＣカード形態の例

【図２５】



コンピュータ・ネットワークへの接続機能付物理乱数発生装置例

【図２６】



記録再生機能付物理乱数発生装置例

フロントページの続き

(56)参考文献　特開　平９－97170（ＪＰ，Ａ）
特開　平５－80987（ＪＰ，Ａ）
特開　平６－259233（ＪＰ，Ａ）
特開　平６－168210（ＪＰ，Ａ）
特開　平４－140947（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.⁶，ＤＢ名)

G06F　7/58
G09C　1/00　650
H04L　9/26
H03K　3/84
H03B　29/00